Reclamation Manual

Directives and Standards

Subject: Reclamation Information Technology (IT) Security Program: Computer Protections, Anti-Virus, Access Control, and Passwords

Purpose: Specifies IT access control, including passwords, and required anti-virus software.

Authority: The Privacy Act of 1974 (5 U.S.C. § 552a); Federal Managers' Financial Integrity Act of 1983 (Public Law 97-255); The Computer Security Act of 1987 (Public Law 100-235); Fiscal Year 2001 Defense Authorization Act (Public Law 106-398) including Title X, Subtitle G, *Government Information Security Reform*; Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Systems* (50 Federal Register 52730, December 24, 1985); OMB Circular A-123, *Management Accountability and Control*, (31 U.S.C. § 3512, June 21, 1995); *Practices for Securing Critical Information Assets*, Critical Infrastructure Assurance Office (CIAO) (January 2000); and Department of the Interior Departmental Manual (DM) Part 375, Chapter 19, *Information Technology Security*.

Contact: Chief Information Office, D-2200

1. **Introduction.** This Directive and Standard establishes authentication, anti-virus software, and computer access control requirements.

2. **Goal.** To ensure adequate access safeguards for computing resources and electronically stored information.

3. **Definitions.**

   A. **Authentication.** A means of identifying or verifying a user or system, ascertaining eligibility to access information and the level of access privileges permitted.

   B. **Password.** A string of alphanumeric and/or special characters used in authenticating an individual or another automated system prior to access of the controlled system, application, or network.

   C. **Access Controls.** Processes of granting access to a network, system, or application, and the authorization of specific predetermined system and information privileges.

   D. **Malicious Code.** Malicious code refers to viruses, trojan horses, logic bombs, and other "uninvited software." Sometimes mistakenly associated only with computers, malicious code can attack other platforms, e.g., routers.

E. **Anti-Virus Software.** Specialized software which detects malicious code and then disables the destructive code before further damage occurs to the computer system or network device.

F. **Smart Card.** A plastic card containing an embedded integrated circuit that can generate, store, and/or process data. It can be used to facilitate various authentication technologies also embedded on the same card.

G. **Biometric System.** An authentication system that utilizes unique physical characteristics that can be converted into digital form and then interpreted by a computer (e.g., fingerprints, voice patterns).

4. **Scope.** This Directive and Standard applies to:

A. All Reclamation-owned, -operated, and -maintained IT systems, including specialized systems (i.e., Supervisory Control and Data Acquisitions Systems, Hydromet, Geographic Information Systems, Dam Safety).

B. All Reclamation-owned IT systems operated and/or maintained by contract or temporary personnel.

C. All Reclamation-owned IT systems operated and/or maintained by organizations or personnel other than Reclamation.

5. **Authentication Requirements.**

A. **Unique Username.**

(1) Every Reclamation employee and contractor will use their own assigned username to log in to all IT systems for which they are authorized. Usernames must be unique and should consist of a user's first initial and last name. When system username length restrictions preclude the use of the entire last name, the last name will be truncated to be consistent with system requirements. When the username has already been assigned, e.g., John Jones as jjones, and Janice Jones needs a username, it is acceptable to use the first letter of the middle name, or include the first two letters of the first name to maintain uniqueness.

(2) Other technologies such as biometric systems and smart cards may be used in place of a username when approved by the system accrediting official. The system accrediting official must determine that the alternative technology is technically equivalent or superior to unique username identification.

B. **Passwords.**

(1) Passwords are required for access to all Reclamation networks. IT systems require passwords if not adequately protected by access controls at the network level. More critical or sensitive IT systems and applications may require additional levels of passwords for increased security. IT systems specifically designated as public (e.g., web servers), do not require "user-level" passwords; however, information and applications on such servers must still be protected from corruption or exploitation. Remote access connections may require additional identification keys and/or processes per individual system security requirements. The combination of a unique username and password is the primary key to positive identification of an authorized Reclamation user.

(2) The initial authentication for user access to Reclamation applications is through a Reclamation network and/or IT system. The application owner will evaluate the necessity for additional security following a risk assessment of the application or application design and incorporate appropriate authentication controls in the system security plan. If an additional level of authentication is required, the application will comply with the standard username and password requirements as described in this Directive and Standard.

(3) Other technologies such as biometric systems and smart cards can be used to replace password requirements, when approved by the system accrediting official as technically equivalent to password protections.

(4) Reclamation passwords will adhere to the following rules and principles:

(a) Passwords will be at least eight characters long. For the operating systems that do not support eight characters, users must use the maximum number of characters allowable.

(b) Passwords will contain no proper nouns, geographic locations, common acronyms, slang, "make believe" words from books or movies, or common English and/or foreign dictionary words.

(c) Cyclical patterns for passwords are not allowed.

(d) Maximum password duration will be 90 days. Exceptions will be approved by the Regional ITSM in writing. Shorter durations are encouraged for more sensitive systems or those exposed to greater threats.

(e) Passwords will contain alpha, numeric, and printable special characters as allowed by the system/application. Allowable special characters will be defined in system-specific security plans or operating procedures. Numeric characters will not be the first character in the password.

(f) Users are not to share passwords for any Reclamation application or system. Operational infrastructure systems, such as multiple remote terminal units or programmable logic controllers deployed at a single site, may be exempt from this requirement. This exemption should be approved by the system accrediting official and documented in the system security plan.

(g) The use of passwords embedded in applications (i.e., automated logins) is allowed only when the user's access is first authenticated through the network using a challenge and response username/password process.

(h) Default passwords on vendor-supplied software will be changed upon installation.

(i) Passwords are not to be disclosed to peers, supervisors, etc., except for emergency access or repairs approved by the system owner. Passwords will be changed immediately after emergency access or repair is completed. Passwords may need to be stored in sealed envelopes in secured locations to address emergency procedures.

(j) A password cannot be used more than once a year. A user's previous five passwords cannot be reused.

C. **Access Controls.** Access controls will be installed and carefully controlled on all Reclamation servers and networks. Authentication will positively identify users prior to authorizing privileges.

(1) Systems will limit the number of consecutive unsuccessful login attempts to three. When these attempt opportunities have been exhausted, the system will disconnect the prospective user. The system will not permit any further attempts against that specific account for at least 15 minutes unless the system administrator intervenes. Systems without this capability must have access controls sufficient to prevent unlimited login attempts and these controls must be approved by the accrediting official in the system security plan.

(2) Access will require a unique username and password or other authorized authentication mechanisms such as smart card or biometric technology.

(3) The following Department of the Interior warning banner will be displayed on all IT systems. Operational infrastructure systems, such as remote terminal units or programmable logic controllers, may be exempt from this requirement. This exemption should be approved by the system accrediting official and documented in the system security plan.

****WARNING TO USERS OF THIS SYSTEM ****

This is a United States Government computer system, maintained by the Department of the Interior, to provide Official Unclassified U.S. Government information only. Use of this system by any authorized or unauthorized user constitutes consent to monitoring, retrieval, and disclosure by authorized personnel. USERS HAVE NO REASONABLE EXPECTATION OF PRIVACY IN THE USE OF THIS SYSTEM. Unauthorized use may subject violators to criminal, civil, and/or disciplinary action.

(4) Remote access users will not leave a system logged in to a Reclamation system/network unattended.

(5) Desktop systems will activate password-controlled screen savers when left idle for 10 minutes or less. Workstations in controlled-access environments or those utilized in the real-time control or display of system information may be exempt from this requirement. The exemption should be approved by the system accrediting official and documented in the system security plan.

(6) Access to specific systems, accounts, applications, and data files will be determined and controlled on a “need to know” basis as determined by the system owner. Users should not be granted access rights to systems or information without a clearly defined “need to know.”

(7) System control privileges will be tightly controlled by system owners. Users will have the least amount of privileges/rights required to perform their assigned duties.

(8) The system-specific security plan will address system access controls.

(9) Unnecessary accounts should be disabled on all systems, e.g,. guest accounts.

D. **Access Termination.** A Federal employee or contractor who terminates employment, is transferred, or no longer has a need to access Reclamation's IT systems, must complete termination procedures using form 7-2205, Computer Access Termination.

E. **Computer Virus Protection.** All Reclamation laptop and desktop systems, work stations, and servers that are capable of running anti-virus software will do so at least weekly. Wherever possible, anti-virus software will have a shield capability to provide continuous scanning of newly added data and e-mail files. Anti-virus software must be addressed in the system security plan which is approved by the system accrediting official. Updates to the anti-virus software's definition files will occur automatically if possible. Laptop and Government-owned, work-at-home computers, which typically are not connected to a Reclamation local area network (LAN), are required to update anti-virus definition files and engines the day of assignment when the device is used regularly or when the machine is assigned to an infrequent user so that the most current versions are installed and available for mandatory use. Users will delete e-mail from questionable or unknown sources in order to avoid possible macro-virus or other contaminations.

6. **Responsibilities.**

A. **Chief Information Officer (CIO).** The CIO has overall responsibility for the IT Security Program in Reclamation.

B. **Accrediting Officials.** Accrediting officials are management officials that are responsible for the overall security and proper use of their IT systems. Directors of Reclamation Regions and Offices have this responsibility for the IT systems under their authority. This responsibility may be delegated no more than one level down (Deputy or Assistant Directors).

C. **System Owner.** The system owner represents the interests of the user community. The system owner serves as the primary functional sponsor/representative for the IT system throughout the system's life cycle. The system owner is responsible for identifying appropriate system security controls. In Reclamation this responsibility is at the Division Chief or Area Office Manager level.

D. **Reclamation's Information Technology Security Managers (ITSM).** ITSMs are responsible for the formation and coordination of computer protection, anti-virus, and access control procedures and processes. ITSMs verify that these processes are adequate, appropriate, and support Reclamation-wide IT security policy, directives, and standards. In addition, ITSMs verify compliance with security architecture restrictions and requirements. The Regional ITSM will coordinate with the appropriate Office/ Regional Director and the Bureau ITSM.

E. **System Administrators.** System administrators have responsibility for establishing user accounts, maintaining system access controls, and configuring systems to ensure password compliance.

F. **Users.** Users have the responsibility to avoid introduction of computer viruses. Users will avoid installing software from questionable sources and reading media without assurance of content. All users will scan electronic media for viruses with the anti-virus software before attempting to use the media. It is the user's responsibility to take known and reasonable measures to ensure the integrity of all data stored or produced on assigned computers and to report security incidents to their managers.

7. **Related Directives and Standards.** For related and supporting Directives and Standards see the Information Resources Management (IRM) section of the Reclamation Manual.